IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 2, 2018, accepted September 17, 2018, date of publication September 28, 2018,
date of current version October 19, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2872115

Masquerading Attacks Detection in Mobile Ad Hoc Networks

SOHAIL ABBAS[1], MOHAMMAD FAISAL[2], HASEEB UR RAHMAN[2], MUHAMMAD ZAHID KHAN[2], MADJID MERABTI[1], AND ATTA UR REHMAN KHAN[3], (Senior Member, IEEE)

[1]Department of Computer Science, College of Sciences, University of Sharjah, Sharjah 27272, United Arab Emirates
[2]Department of Computer Science and IT, University of Malakand, Chakdara 18800, Pakistan
[3]Faculty of Computing and Information Technology, Sohar University, Sohar 311, Oman

Corresponding author: Sohail Abbas (sabbas@sharjah.ac.ae)

ABSTRACT Due to the lack of centralized identity management and the broadcast nature, wireless ad hoc networks are always a palatable target for masquerading attacks. The attackers can spoof identities of privileged legitimate users for various malicious reasons, such as to launch DoS or DDoS attacks, to access unauthorized information, and to evade the detection and accountability. In the current and limited literature, masquerading attacks are mostly counteracted by signal-strength-based detection systems. However, these schemes are mostly proposed to work for infrastructure-based IEEE 802.11 wireless networks using fixed access points, air monitors, or fixed anchor nodes, which are not suitable for the *ad hoc* architecture. In this paper, we propose a detection system for masquerading attacks without using fixed anchor nodes or air monitors. We develop an anomaly detection model based on the statistical significant testing for our masquerading detection system that takes into consideration the signal strength fluctuation. We conduct a test bed of Samsung Galaxy-based smartphones in order to analyze the real-world signal strength variation. We also plug the real-world signal strength variation in our model for the evaluation of the detection accuracy. We propose the received signal-strength-based masquerading attack detection scheme, which is carried out first by each node in its one-hop vicinity and then extended to five-hop proximity for broader detection scope and improved accuracy. The proposed scheme is evaluated using an NS-2 network simulator for detection accuracy in different environments. The results obtained indicate that our proposed scheme produces more than 90% true positives.

INDEX TERMS Masquerading, spoofing attack, intrusion detection, mobile ad hoc networks.

I. INTRODUCTION

Unlike regular wireless networks, such as cellular networks and WiFi, the Mobile Ad-hoc Networks (MANETs) may be deployed without any pre-installed infrastructure or centralized administration in self-organized manner. Since these networks do not rely on any pre-installed architecture, they are less costly and can be used in situations like earthquake, floods, battlegrounds, search and rescue operations etc. Other, non-emergency, applications include, wireless sensor networks, vehicular ad hoc networks [1], robot networks, unmanned aerial vehicles [2], underwater networks, Internet of Things (IoT) [3], and so on. One of the future prospects in commercial applications' setup is that the IoT paradigm and 5G would enable the integration of fixed infrastructure with the ad hoc architecture in order to constitute a heterogeneous environment [4]–[6].

Usually, the network entities, such as nodes, base stations and access points are identified by unique identifiers, and each physical network entity must follow a one-to-one mapping of an identity and an entity (i.e. a node). However, in MANETs, this one-to-one mapping of identity and entity is hard to impose due to their open nature, distributed architecture, and absence of identity management systems. Hence, malicious nodes violate this identity-entity mapping while creating two problems thereby compromising, i) entity distinctness and ii) identity uniqueness. In the former case, the identities are unique but they are not referring to distinct entities or nodes. For example, in case of Sybil attacks [7], the attacker can forge more than one identity on a single physical device. Hence, these fake identities (no matter if they are unique) in reality refer to a single distinct node in the network. These attacks can also pose various threats to various

protocols discussed in [8]. For instance, Sybil attacks can create multiple identities to disrupt voting based protocols, location based protocols, or protocols developed for shared resources. In our previous work [9], we have proposed solution for this case. In the latter case identity uniqueness is compromised, i.e., entities or nodes are distinct but the identities representing them are no more unique. For example, an attacker can forge already existing identities; hence, creating a situation where two or more than two identical identities will exist in the network simultaneously representing distinct entities, known as masquerading or identity spoofing attack [10]. The broadcast nature of wireless networks enables attackers to collect useful identity related information, such as MAC address via passive monitoring. These identity related information can then be used by the attackers to launch masquerading attacks. These sort of attacks in which identity is compromised can pose serious threats to the overall network operation. For example, an adversary can request services, for which it is not authorized. Similarly, an attacker can launch other types of attacks, such as malicious traffic injections, information fabrication, DoS or DDoS without the fear of being get caught or detected. These attacks also promote lack of accountability in the network. Masquerading attack detection is a challenging problem and it is also difficult to prevent it in wireless ad hoc networks because of the open nature and lack of centralized identity management and control.

The lightweight and distributed solutions are always tempted for ad hoc networks. One path towards this is to exploit those properties of the network that cause low overhead and fewer changes to the existing system and that properties may not be manipulated even when the nodes are compromised. Recently, the researchers use a property of nodes, called Received Signal Strength (RSS) which is related to the transmission and reception of the communication signal. The RSS is a lightweight alternative to cryptographic based authentication which also does not require any additional costs to the existing wireless technology. However, the RSS is not quite reliable because it varies and fluctuates over time due to various factors, such as multipath fading, reflection, refraction, etc. However, it can still provide promising and acceptable accuracy in wireless environment, as we will show in the coming sections.

Various authors, such as [10]–[14] proposed solutions for the masquerading attack detection based on RSS. However, those schemes are developed either for infrastructure based wireless networks, in that case fixed access points or air monitors were used to record RSS readings or for ad hoc networks where fixed anchor nodes were used for the same purpose.

In this paper, we propose a technique for masquerading attack detection in mobile ad hoc networks, when an attacker forges and takes on the already existing identities, causing an anomalous situation; i.e. the existence of an identity at more than one location in the network at the same time. Our proposed technique is RSS based and does not rely on fixed anchors or any extra hardware, such as GPS or directional antennae. We use the distance parameter (in physical space as a result of the RSS in signal space) for the attack detection.

The rest of the paper is organized as follows. In Section 2, we discuss the related work proposed in the literature. In Section 3, the proposed detection technique is presented with the design rationale and the theoretical detection model which is built using statistical significant testing. In Section 4, the proposed detection system is discussed. Section 5 encompasses the simulation based evaluation of the proposed detection system using various metrics. Finally, the paper is concluded in Section 6.

II. RELATED WORK

One of the main approaches used to counter the spoofing and other identity related attacks is to use a trusted Certification Authority (CA) [15]–[17]. Some authors use centralized CA while some customized the approach for the distributed architecture of ad hoc networks and proposed distributed CA based techniques, such as [18]. Some authors proposed self-certified CA systems where nodes can generate identities for themselves as many required [19], [20]. No matter the centralized or the distributed CA is in place, the responsibility of these schemes is to create, maintain, and revoke identity certificates for each network identity. One of a good example of such schemes is the scheme proposed by Seth and Keshav [21] in which a concrete cryptosystem for ad hoc networks has been proposed focusing on Hierarchical Identity Based Cryptography (HIBC). In their approach the authors plugged the anonymity into their technique. Their technique is scalable because it is semi distributed forming hierarchies where nodes can freely roam across the network. However, these CA based approaches suffer from various problems. First, these schemes rely on heavy asymmetric cryptography. Second, the CA needs to be accessible to all nodes in the network, all the time. Third, it is not clear that how a trusted CA will be selected and for how long it will play this role. Fourth, what will happen if the designated CA leaves the network becomes faulty or gets compromised? Chuang and Lee [22] addressed some of these issues but at the cost of extra hardware, i.e. tamper-proof, TPM (Trusted Platform Module) for each network node. Further discussion on this topic is out of the scope of this article, interested readers are referred to [23] and [24].

A wide range of schemes focuses on a problem when an attacker (such as Sybil attacker) forges fake (non-existent) arbitrary identities in the network. The stance of these schemes is to detect and counter multiple identities created on a single physical device, i.e. Sybil attack [7]. In other words, they are analyzing whether more than one transmission are received from same location while disguising different identities, which implies, multiple identities at one location. This is entity distinctness case, already discussed in the preceding section. These schemes generally use received signal strength indicator, radio resource testing, and position verification mechanisms in order to detect and counteract Sybil attacks,

examples of such schemes are [9] and [25]–[28]. For further details on this topic, readers are encouraged to read [29] and [30].

Misra *et al.* [11] proposed an RSS based spoof detection method for wireless sensor network. Multiple monitoring nodes cooperatively analyze the change occurred in the received signal strength at each site in order to detect the attacker. The author only relied on the simulation without conducting any testbed experimentations.

Yu *et al.* [12] proposed a framework for IP and MAC addresses based spoofing attack detection, in which they used the network characteristics, such as RSS, and developed proximity-based access controls for the victim's house. The scheme suffers from its limited scope, i.e., the fixed threshold for the house and any request coming from outside is deemed as an attacker.

Chen *et al.* [13] and Yang *et al.* [31] proposed a method of detecting Sybil attacks and spoofing attacks and then localizing them in the infrastructure based WiFi and wireless sensor network environment. Fixed landmarks and dedicated anchor nodes were used to collect and analyze the RSS readings from the nearby nodes which were used to detect and localize the attackers.

Sheng *et al.* [14] proposed RSS based scheme to detect spoofers that exploit MAC addresses in the 802.11 wireless LANs. The author also considered the rogue access point problem in which a malicious node impersonates a legitimate WiFi access point in order to trick the normal users. The RSS readings' pattern was analyzed in a 3-floor building covered by 20 air monitors using their proposed Gaussian mixture model. The results are interesting, however, in ad hoc mode the inclusion of air monitors will be impractical to install.

Faria and Cheriton [32] demonstrated that attackers could be identified by their transmitting devices' signal prints which is basically a tuple of signal strength values recorded at multiple access points. The detection was performed based on per packet, i.e., each packet was tagged with its source's signal print which was further analyzed for possible attack. The scheme relied on the fixed access point for the overall detection.

Similar to the previous scheme, the work in [33] and [34] also use signal prints for detection; however, the author used data mining techniques and artificial neural networks for signal clustering. While in the same context, [10] used Naïve Bayesian classifier.

III. PROPOSED TECHNIQUE

In this section, we will use the RSS property of wireless communication to detect the spoofed identities. In order to analyze the malicious nodes' activities, RSS will be recorded from them by their 1-hop neighbors. We believe that malicious nodes must be involved in some sort of communication with their victims, such as downloading, uploading, etc. Therefore, in our scheme, each node monitors and records all direct and overheard frames (i.e., IEEE 802.11 protocol frames: rts, cts, data and ack) from its 1-hop neighbors.

TABLE 1. Neighbour list based on RSS.

Node ID	Rss-List
1	R1 | T1 → R2 | T2 → R3 | T3 - - - - - ≫ Rn | Tn
2	
3	
. . .	
N	

This information will be stored in a table form, i.e. <Address, Rss-List <time, rss>>, as shown by Table 1.

The number of elements in the Rss-List can be adjusted depending on the memory requirements.

A. SOLUTION RATIONALE

The main point of the rationale is that no two distinct nodes can mimic their movement and communication patterns over time. In other words, two identical but distinct nodes, if analyzed properly, may not follow 100% same movement and communication pattern. For example, consider Figure 1, if a monitor node x analyzes the movement and data transmit pattern of both the duplicate identities, i.e., m and m', over a time period t, these may not be able to sustain such mimicry and impersonation. In order to analyze the movement pattern, each node will assess the received RSSs captured from the same identity. Let R_i^j be the RSS of node j received at node i. As shown in Figure 1, let m and m' be identical identities, i.e., one is victim and the other is masquerader, both lying at distance d_1 and d_2 from node x, while $d_1 \neq d_2$. In situation where there is no mobility, node x can detect the attack if $R_x^m \neq R_x^{m'}$. However, if nodes are mobile, this trivial

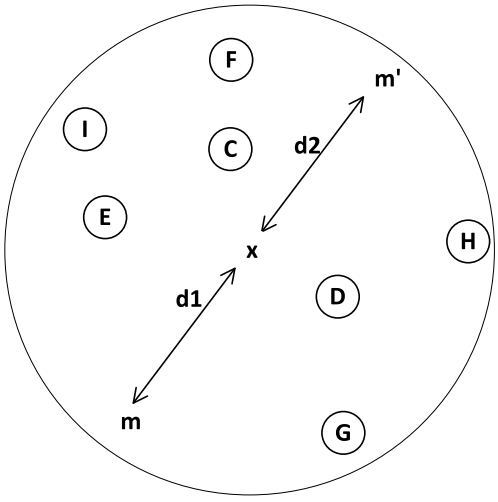

FIGURE 1. Masquerading attack scenario.

comparison may not help in detection. There may not always be an attack situation, for instance, a genuine node can change its location due to mobility or switched-off in one place and switched-on on another location. In other words, using the monitored RSS, the receiver needs to determine whether the messages are received from one legitimate node moved from one location to another or from two distinct nodes lying at two different locations (attack situation). For example in Figure 1, if the nodes are mobile, node x receives frame $f1$ and $f2$ at time $t1$ and $t2$, respectively from an identity m. Now, the job of node x will be to find out whether the received messages are from a legitimate node moved from location $l1$ to $l2$ or that are from two distinct nodes (i.e. m and m').

In order to detect this situation, we include two things in our detection mechanism. First, time of reception is included with each RSS received. For example, $R_i^j(t_k)$ be RSS of node j received at node i at time t_k. Following this notation, node x can compute change in RSS for node m, i.e. $\Delta R = R_x^m(t_k) - R_x^{m'}(t_{k-1})$. Second, we assume that the maximum speed[1] nodes may attain in the network is V_{max} ms^{-1}. And let R_{max} be the change induced in the signal space when a node covering distance $d_{\max}$ (i.e. the distance covered by a node moving from location $l1$ to location $l2$ with $V_{\max}$) in Δt time interval. As a result, a transmitter may never induce a change (in the form of RSS) greater than that of the R_{max} at a receiver. This is due to the fact that no node may travel more distance than the $d_{\max}$ in a Δt time interval.

In order to map the ΔR to its equivalent distance in physical space, we use Equation 1 which implied that the received power at distance d, denoted by P_d, is inversely proportional to the lth power of distance d.

$$P_d \propto \frac{P_t}{d^l} \tag{1}$$

Where d is the distance between transmitter and receiver, l is the path loss exponent and its value depends on the environment. For Line-of-Sight (LoS) and free space conditions, its value is 2 and for other environments, such as indoor with obstacles, its value is usually greater than 2 [35]. The received power at any distance d and reference distance d_0, for $d > d_0$, will be $\frac{P_d}{P_{d_0}} = \frac{d_0^l}{d^l}$, and after taking its logarithm, we get Equation 2.

$$P_d\,(dbm) = P_{d_0}\,(dbm) - 10\log_{10}\left(\frac{d}{d_0}\right)^l \tag{2}$$

$$\Delta d = 10^{\left(\frac{-\left(P_{\Delta R} - P_{d_0}\right) + 20\log_{10}(d_0)}{20}\right)} \tag{3}$$

[1]This assumption is valid because in some networks, such as vehicular ad hoc networks, it is possible to determine the maximum possible speeds of nodes based on the fastest car speed meter or the permissible speeds limits on roads. Similarly, the maximum speed of IEEE 802.11 based network nodes inside a building will be hardly 1 to 3m/s because nodes (laptops or smart devices) might be carried by humans walking inside the building.

The distance can also be calculated without the reference distance as shown in Equation 4

$$\Delta d = 10^{\left(\frac{R_A^m(t_k) - R_A^m(t_{k-1})}{20}\right)} \tag{4}$$

The detector nodes will check the relation given in Equation 5. Any change in RSS greater than a threshold, Γ, will be considered as an attack. The threshold Γ can be calculated as $\Gamma = V_{max} * \Delta t$.

$$Detection = \begin{cases} \Delta d > \Gamma & Attack \\ \Delta d \leq \Gamma & Normal \end{cases} \tag{5}$$

To summarize the implication of Equation 5, node x will analyze ΔR (also mapping it to distance, Δd) over time Δt. If the change incurred during Δt is greater than the maximum possible change (i.e., Γ), m will be considered as malicious, otherwise normal node. If we consider only movement of these nodes, there are three possibilities which are analysed below:

(i) Both m and m' are static: if both of these nodes are static, the detection is quite easy. They will induce dissimilar RSS at node x. However, if both of these nodes are at the same distance from the node x and both of them are static over time, then it will not be detected by x, and hence, a false negative ensued. The reason for this false negative is that these nodes are static over time and lying approximately at the same distance from x, as a result they cannot induce significant change at x. However, this situation may not happen to every detector node, for instance, m and m' may not be at the same distance or angle to other neighbors, i.e., node y, and will be detected by those neighbors.

(ii) Both m and m' are mobile: the detection in this case is also quite plausible because since both of these nodes are mobile, they cannot follow the same movement pattern; hence they will be detected.

(iii) m is static while m' is mobile or vice versa: if at least one node is changing its moving pattern (i.e. location) will ultimately change the distance between m and x or m' and x; hence will be detected.

B. THEORETICAL DETECTION MODEL

The RSS is influenced by various factors, such as obstacles, multipath effects, random noise, etc. However, it still presents a strong relationship and mapping with distance [36]. It is observed during our testbed experiments (next sub-section), that the RSS's collected at various locations are distinctive.

In spite of RSS's several-meter accuracy, it is still an attractive choice for various detection and localization systems. One of the main advantages of using RSS in such systems is that it is a physical property of wireless communication that is lightweight in nature and that is the reuse of the existing infrastructure. Furthermore, it can still fulfill the accuracy requirements of the aforementioned systems.

In order to tune the Γ threshold, in the presence of RSS variation, for improved accuracy, we theoretically analyze the

signal space of a static node. This will help in determining node distinguishability for our detection system.

The aim of this section is to theoretically analyze how accurately two nodes (as close to each other as possible, lying on a straight line) can be detected in the presence of RSS variation. We propose an RSS based detector to detect the presence of the spoofing attack. Normally, each location is bound by a single identity. Let a receiver node receives R signal strength readings from a transmitter node during the observation period T_{obs} that maps to distance d_1. As we will see during our testbed experiment that R follows standard normal distribution with mean, μ_R. If the mean μ_R changes enough to map to distance d_2 (another distinct location), the receiver node would tag the transmitter node as attacker. At the receiver, when signal space of an identity is mapped to its physical space, the normal situation would be $d_1 = d_2$; whereas, $d_1 \neq d_2$ will be considered as an attack. So, in simple terms, significantly different RSSs received from same identity implies same identity at more than one location; hence, an attack is assumed. In order to check how significant the change in RSS is, based on which we can claim that the difference in RSS leads to the attack, we formulate the detection of the attack as a classical statistical testing problem, i.e. significant testing using null hypothesis, where the null hypothesis is

$$\mathcal{H}_0 \colon \ \mu_R = 0 \, (d_1 = d_2 \colon \ no \ atttack)$$

and the alternative hypothesis is

$$\mathcal{H}_1 \colon \ \mu_R > 0 \, (d_1 \neq d_2 \colon \ attack) \, .$$

We will take test statistic T that is used to assess the RSS sample(s) whether they belong to the null hypothesis or alternative hypothesis [37]. Let α is significance level, which is the probability of rejecting the H_0 if it is true (this is also called type I error), and there is an acceptance region Ψ and critical region Ψ_c such that if the observed data $T_{\text{obs}} \in \Psi$ the null hypothesis is considered as accepted and rejected otherwise. In case of rejection, we would say that $T_{\text{obs}} \in \Psi_c$.

We rewrite Equation 1 in the form of log-normal shadowing model that predicts path loss as a function of transmitter-receiver separation, we get

$$P_d \, (\text{dBm}) = P_{d_0} \, (\text{dBm}) - 10 \log_{10} \left(\frac{d}{d_0} \right)^l + X_\delta \qquad (6)$$

Where P_d is the received power (RSS) at distance d, P_{d_0} is the transmit power of a node at a reference distance d_0 and d is the distance between the sender and the receiver. l is the path loss exponent and its value varies from environment to environment [35]. The X_δ is zero-mean Gaussian random variable, also known as the shadowing factor with $\delta/\sqrt{2}$ standard deviation [38]. Assuming homogeneous transmit power, the observed change in the RSS at the receiver is given by

$$\Delta P = 10 \log_{10} \left(\frac{d_2}{d_1} \right)^l + \Delta X \qquad (7)$$

Eq-7 may help in developing a threshold that will distinguish between the legitimate and masquerading nodes. That is, we can analyze the RSS computed in Eq-7 in both cases, i.e. when d_2 and d_1 are same (which would mean RSS emanated from same location) and when d_2 and d_1 are not same (which would imply RSS emanated from different location). In the former case, the RSS follows a normal distribution with zero mean and $\delta/\sqrt{2}$ standard deviation. In the latter case, the RSS follows a normal distribution with $10 \log_{10} \left(\frac{d_2}{d_1} \right)^l$ mean and $\delta/\sqrt{2}$ standard deviation. Equation 8 and Equation 9 depict the probability density functions of the above mentioned two cases; which can also be seen diagrammatically in Figure 2.

$$f \, (\Delta p | d_2 = d_1) = \frac{1}{\sqrt{2\pi}} e^{\frac{-p^2}{2\delta^2}} \qquad (8)$$

$$f \, (\Delta p | d_2 \neq d_1) = \frac{1}{\sqrt{2\pi}} e^{\frac{-\left(p - \log_{10} \left(\frac{d_2}{d_1} \right)^l \right)^2}{2\delta^2}} \qquad (9)$$

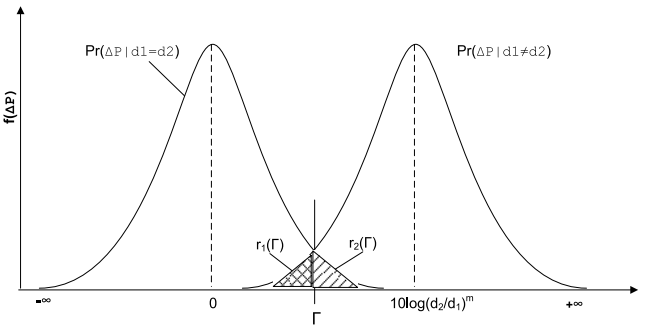

FIGURE 2. ***pdfs*** **of attack and normal situations.**

Let Γ be the signal space threshold that can distinguish between the RSS originated from same location or different location. We use Type-I and Type-II errors from the hypothesis testing formulation in order to determine the detection accuracy, i.e. True Positive (TP) and False Positive (FP) rates. The TP is the probability that the two nodes are at different locations based on the RSS distribution (called power of the test), can be given as:

$$\begin{aligned} TPR &= \Pr \left(\Delta p > \Gamma | d_2 \neq d_1 \right) \\ &= 1 - \Gamma \left(\frac{\Gamma - 10 \log_{10} \left(\frac{d_2}{d_1} \right)^l}{\sigma / \sqrt{2}} \right) \end{aligned} \qquad (10)$$

Whereas, the FP rate can be given as

$$FPR = \Pr \left(\Delta p > \Gamma \, | \, d_2 = d_1 \right) = 1 - \Gamma \left(\frac{\Gamma}{\sigma / \sqrt{2}} \right) \qquad (11)$$

The $\Gamma(\cdot)$ is the cumulative density function of the standard normal distribution.

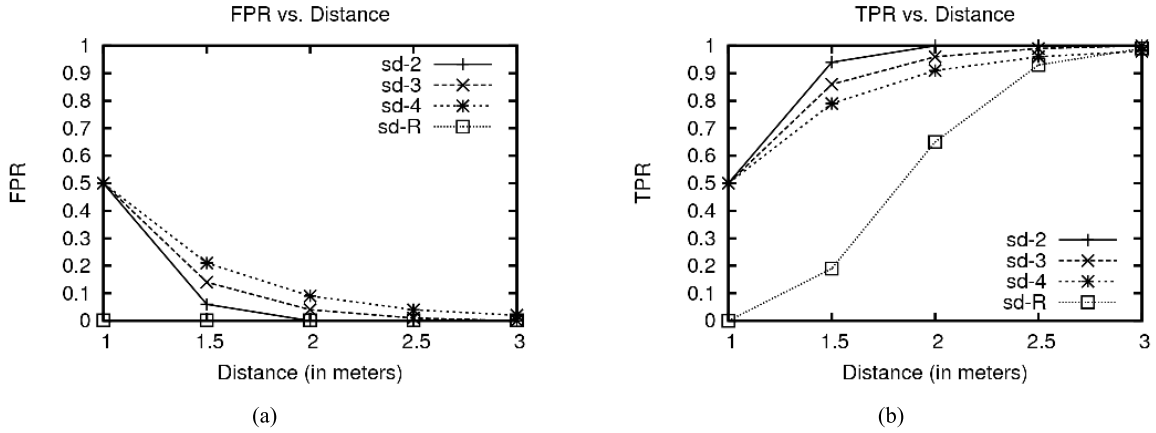

FIGURE 3. The relationship between distance and detection accuracy: (a). False positive rate and (b). True positive rate w.r.t distance.

As depicted in Figure 2, the probabilities of erroneously classifying the RSS in the two cases may be written as

$$r_1(\Gamma) = \int_{-\infty}^{\Gamma} f(\Delta p|d_2 \neq d_1)ds \tag{12}$$

$$r_2(\Gamma) = \int_{\Gamma}^{+\infty} f(\Delta p|d_2 = d_1)ds \tag{13}$$

$$r_t(\Gamma) = r_1(\Gamma) + r_2(\Gamma) \tag{14}$$

In order to determine the threshold that produces the minimal error rate, we differentiate $r_t(\Gamma)$ with respect to Γ and equating it to zero, we get

$$f\ (\Gamma|d_2 = d_1) - f\ (\Gamma|d_2 \neq d_1) = 0 \tag{15}$$

By solving Equation 15 for Γ and substituting Equation 8 and Equation 9 into it, we can get the optimum threshold, i.e.,

$$\Gamma = 5l \log_{10}\left(\frac{d_2}{d_1}\right) \tag{16}$$

Figure 3 shows the detection accuracy for various distances using Γ as the detection threshold. Different standard deviations are also considered for different signal fluctuations. It is quite evident in the figure that the detection accuracy is affected by the signal fluctuation and separation distance. For instance, the closer the two nodes are, the worst is the detection, i.e., low True Positive Rate (TPR) and high False Positive Rate (FPR). The TPR is increased to more than 95% with less than 5% FPR when the separation distance reaches 3 meter. Similarly, the signal variation also affects the detection accuracy, for example the lower the standard deviation, the better the detection accuracy. In our analysis, sd-2, sd-3, sd-4 are used as 2, 3 and 4 standard deviation of the RSS respectively. Nevertheless, our concern is also to determine the actual real world signal fluctuation in the RSSs, for which we performed an experiment to collect and analyze the RSS captured at various distances.

During our empirical analysis, we observed that the farther the transmitter the greater the variation in the RSS. For coping with the worst case situation, we considered the case when the transmitter is 60ft or 18.3m apart, the recorded standard deviation is 3.3. For 95% confidence interval, i.e., 2SD, we used sd-R as real world observed standard deviation; the results can be seen in Figure 3. The detection is still better because it produces more than 95% TPR around 3m distance separation with low FPR. In spite of this 3m distance gray zone, our proposed scheme will still be a striking choice for various reasons in multiple domains. First, our approach is only reusing the existing wireless equipments. Second, our scheme fulfills the accuracy requirements of almost all of the applications. For instance, in Vehicular Ad hoc Networks (VANETs), the vehicle dimensions are more than 3m and any malicious vehicle will easily be detected by our scheme. Similarly, in health care domain, a doctor who monitors patients may only be interested in the rooms where the patients' reside.

C. TESTBED CONDUCTION

The RSS is considered to be unreliable property over time, as pointed out by many authors such as [30] and [39]. Therefore, it is strongly recommended to analyze the real-world RSS readings and its fluctuation. The aim of this testbed would be to analyze upper bound of the fluctuation incurred in RSS in worst cases, such as boundary conditions. For this purpose, we conduct a testbed of smartphones in indoor environment (however, we tried to avoid any obstacles in the line-of-sight). We use smartphones because they have longer radio ranges and also they are widely being used. We use Samsung Galaxy S6 smartphone embedded with 1.5GHz octa-core Samsung Exynos 7420 processor and with 3GB of RAM. We setup the transmitter and receiver to collect RSS readings from three different distances, i.e. 1ft, 30ft and 60ft. During our empirical analysis, 1000 RSS samples were collected at each location. The descriptive analysis of these distances can be seen by Figure 4 and Table 2. It can

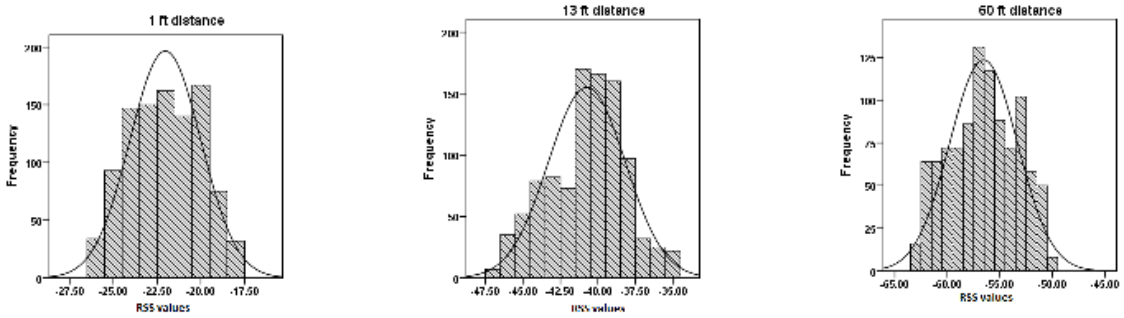

FIGURE 4. Frequencies distribution of RSS at 1ft, 30ft and 60ft distances.

TABLE 2. Descriptive Statistics taken of RSS at three distances, 1ft, 30ft, and 60ft.

	N	Minimum	Maximum	Mean		Std. Deviation	Variance
	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Statistic
1-ft	1000	-26.00	-18.00	-22.0320	.06416	2.02906	4.117
30-ft	1000	-47.00	-35.00	-40.7370	.08134	2.57225	6.616
60-ft	1000	-63.00	-50.00	-56.5550	.10210	3.22884	10.425

be observed that there is considerable amount of fluctuation in the RSS which increases with increase in distance between transmitter and receiver nodes, see the increase in variance or standard deviation with the increase in distance between the transmitter and the receiver in Table 2. In worst case, i.e. at the boundary (60ft), the RSS incur 3.3 Standard Deviation and for 95% confidence interval this will become double. We have plugged this value in the Figure 3 above.

IV. THE PROPOSED DETECTION SYSTEM

In Section 3, we proposed solution for masquerading attack detection in the 1-hop vicinity which suffers from two problems. First, the detector node's view is restricted and it does not know the masquerading identities beyond its radio range. Second, an attacker may not be detected if the attacker's and victim's movement pattern do not cause the change in RSS greater than that of the threshold Γ. In this section, we will discuss how to strengthen our proposed scheme to counteract these issues. We use the 1-hop RSS information gathered by each node in extending the knowledge of malicious identities beyond the native radio ranges. This equip each detector node with the ability to monitor the attack in a broader range, i.e., up to 5-hop vicinity (two hops on both side of a node in a line) and also with the improved detection. In order to formulate the problem, we devised a scenario in the form of a grid topology for simplicity reasons, as shown in Figure 5. Let the dotted circle around node 0 is its radio range encompassing four nodes. In this nodes' setup, without losing symmetry, each node has four 1-hop neighbors, as shown. Suppose that there is a masquerading identity in the 2-hop neighborhood of node 0, i.e. Id 8' shown by solid dotted line. Since, it may be detected by node 3 as per our previous proposed scheme. However, if somehow due to the above mentioned reasons, the detection is delayed or could not take place at all, the attacker may get a chance to carry out its malicious activities. In order to strengthen our previously proposed scheme, we propose an add-on to it in this section.

A. PROCEDURE

Each node periodically broadcasts the RSS readings recorded from its 1-hop neighbors, in the form of a template $T < T_r, R_v, R_i, t_i >$. Where T_r and R_v are the transmitter and receiver addresses respectively; and R_i is the ith RSS collected at time t_i. In Figure 5(a), node 4 constructs RSS template for its 1-hop neighbors and shares it with its neighbors afterwards. If overhead reduction is the concern, the template T may be piggybacked in the control frames of IEEE 802.11, for example, rts, cts, data, and ack frames. After receiving T, each node will record the R_v nodes as its 1-hop neighbors and the T_r nodes as the 2-hop neighbors in a table. As depicted by Figure 5(b), node 0 fills up the information from the T received from node 4 in its table, excluding its own identity. In order to enable node 0 to monitor indirectly its 2-hop neighbors, it will rely on the information provided by its direct neighbors, i.e. node 1, 2, 3, and 4. Instead of relying solely on the direct neighbors, node 0 can also indirectly confirm the detection. But, how node 0 would find

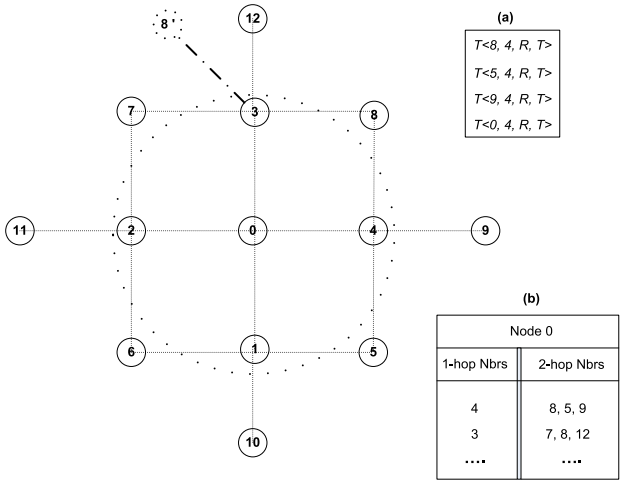

FIGURE 5. General example. (a) RSS template construction. (b) node reachability at 2-hop distance.

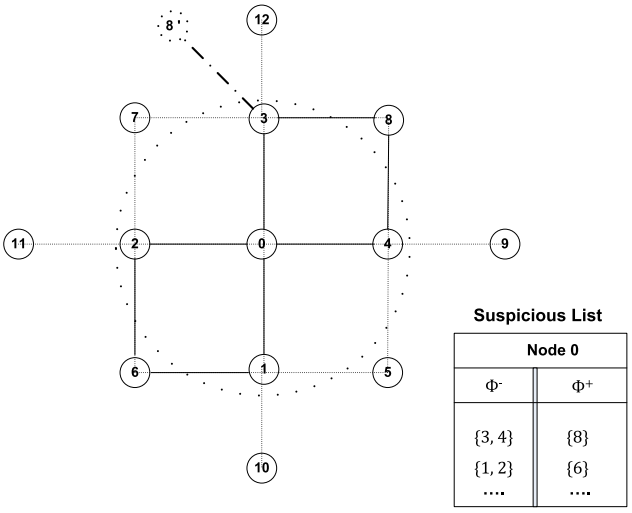

FIGURE 6. Masqueraders and shared neighbors at 2-hop distance.

out whether its direct neighbors, 4 and 3 refer to a single legitimate identity of a distinct shared neighbor 8 or these nodes inadvertently interacted with an attacker, i.e. 8' (which can be seen in Figure 5 with solid dotted line)? In other words, how would node 0 identify such cases from the table given in Figure 5(b), whether identities 5, 6, 7, and 8 are just shared neighbors or masqueraders? This question will be answered in the following subsection after building some formal notations.

B. DETECTION

Let N nodes are uniformly distributed in an area A. For a node x, $n(x)$ are the 1-hop neighbors of node x. Two nodes, x and y, can directly communicate with each other if they are direct neighbors of each other, i.e. if $x \in n(y)$ then $y \in n(x)$. Let $n_2(x)$ be the 2-hop neighbors of x which are basically set of nodes that are neighbors of at least one node of$n(x)$; however, they do not belong to $n(x)$, i.e. $n_2(x) = \{y \,|\exists z \in n(x) | \, y \in n(z) \setminus \{x\} \cup \{n(x)\}\}$. For a node $y \in n(x)$, let $\Gamma_x^+(y)$ be the number of nodes belonging to $n_2(x)$ but also belong to $n(y)$, i.e. $\Gamma_x^+(y) = |n_2(x) \cap n(y)|$. In other words, this quantity denotes the number of $n_2(x)$ nodes which node x can reach in two hops via node y. Similarly, for a node $y \in n_2(x)$, let $\Gamma_x^-(y)$ denotes the number of nodes of $n(x)$ which are also in $n(y)$, i.e. $\Gamma_x^-(y) = |n(x) \cap n(y)|$. In other words, this quantity denotes the number of nodes in $n(x)$ that act as intermediary nodes and make the connection between x and y possible in 2-hops. The Γ^- set of nodes share or broadcast the RSS readings of Γ^+ nodes. These sets can be seen in Figure 6.

If the identities in the set Γ^+ happen to be duplicate ones, they will be put in a suspicious list. For example, node 0 receives messages from 3 and 4 regarding a shared neighbor, i.e. 8, see Figure 6. Since, it is not clear to 0 whether these nodes are referring to the same node or spoofed identities, i.e. identity 8' (shown in dashed circle). Such identities will be put in the suspicious list for observation period t. RSS reading will be analysed for these identities residing in the suspicious list. In case of normal shared neighbor, such as node 6, node 0 will compare the ΔR computed from the templates shared by node 2 and 1 for their shared neighbor, i.e., node 6, which will be almost same. It is due to the fact that the node is distinct; hence, each receiver will record the same transmitting pattern. As a result, records coming from node 2 and 1 will be almost same. Whereas, in attack situation, i.e. node 8 and 8', node 4 records RSS from a single node, i.e. node 8, while node 3 records RSS from two nodes, i.e. node 8 and 8'; hence, the transmit pattern received will be different than that of the node 4. This is how node 0 will distinguish between the shared neighbor and the attacker node. The pseudocode of the process is given below.

Malicious nodes may try to disrupt the detection process by not sharing the RSS readings with neighbors, which will not affect the detection accuracy. Because the system would require evidence against malicious nodes for being detected, which will be provided by the non-malicious nodes.

C. DEALING WITH FABRICATED RSS RECORDS

Malicious nodes can generate and share fabricated RSS records in order to disrupt the detection system or create a DoS situation in the network. It would have been very straightforward if every node uses asymmetric cryptographic based digital signatures that would not only authenticate the identities; but also protect messages from being tampered with by the malicious entities. However, due to their reliance on public key cryptographic based computations and trusted third party, they are not suitable for the resource constraint devices and distributed architecture of mobile ad hoc networks. Alternatively, symmetric cryptographic based techniques run three to four orders of magnitude faster than that of the asymmetric cryptographic operations (i.e. for digital signatures). Hence, in our proposed scheme to protect the RSS readings from being tampered with, we use a symmetric cryptographic based technique, called one-way hash chains [40], [41]. Various authors used one-way hash chains

Pseudocode

```
1. Procedure: AddRSS(src_address, rss,
recv_time)
//src_address is the transmitter
of the rss and recv_time is time of
reception at the receiver.
If(src_address of rss is in
suspicious_list) then
    If(timer_expired ==true) then
      Remove src_address from the
suspicious_list
    EndIf
    Else if(ΔR > Γ)then
    Add src_address to malicious_list
    EndIf
EndIf
If(src_address is not in the
rssTable)then
  Create_record(src_address)
  Add rss and recv_time to src_address
record
  If(no_ofrecords > LIST_SIZE)then
    Pop_front
EndIf
  EndIf
Else
    Map ΔR to Δd
    If(Δd > Γ)  then
      Add src_address to malicious_list
    EndIf
EndElse
2. Procedure: BcastHandler(q, p, rss,
recv_time)
//BcastHandler handles the rss
template shared by 1-hop neighbors.
Input includes: q is 1-hop and p
is 2-hop neighbor having rss with
reception time. child(p) means the
rss linked records attached to p.
If(p is not in bHandler_Table)then
  Create record for p and add q to
child(p)
EndIf
Else If (q is not child(p))then
     Add q to child(p)
   EndIf
EndElse
For each child(p) repeat
     For all child(q) repeat
     If(child(p) == child(q)) then
       //add p and q to suspicious_list
       Add p and q to Φ⁻
       Add child(p) and child(q) to Φ⁺
     EndIf
   EndFor
EndFor
```

to guard against malicious attacks, such as DoS and resource consumption attacks, etc. [41].

A one-way hash chain is usually constructed based on a hash function, H, that maps a variable length input to a fixed length bit string, i.e. $H : \{0,1\}^* \rightarrow \{0,1\}^\rho$, where ρ is the hash function output length (in bits). Examples of hash functions include MD5 [42] and SHA-1 [43]. Some of the properties of an ideal hash function H include:

- H can take an input of any length but must generate a fixed length output.
- For any given input x, $H(x)$ will be easy to compute.
- It will be computationally infeasible to computer x from the function $H(x)$ (one-way property).
- $H(x)$ will not produce identical outputs for two or more same inputs (collision-free property).

In order to create a one-way hash chain, a node selects a random number $x \in \{0,1\}^\rho$ and then computes a list of values based on x, i.e. $h_0, h_1, h_2, h_3, h_4, \ldots h_n$, such that$h_0 = x$, and $h_i = H(h_{i-1})$ for $0 < i \leq n$. The hash chains are initially generated from left to right, i.e. $h_0 \rightarrow h_n$ and these elements of the chain are then used over time from right to left, i.e. $h_n \rightarrow h_0$ in order to secure data. For instance, given an authenticated element of the chain, it is possible to validate the preceding elements of the chain. That is, given an authenticated elementh_n, a node may authenticate h_{n-1} by computing $H(h_{n-1})$ or even h_{n-4} may be authenticated by computing $H(H(H(H(h_{n-4}))))$ and then comparing the results with the h_n.

These chains can be created all at once and each element can be stored before usage. Alternatively, these chained elements can also be computed on-demand. Hybrid approach has also been proposed. Coppersmith and Jakobsson [40] and Jakobsson and Markus [44] proposed a storage efficient solution, i.e. one-way hash chain with N elements would only need $log(N)$ computation and $log(N)$ storage.

We will use the above mentioned one-way hash chains in order to protect the RSS readings from being fabricated at the time of dissemination. To use the one-way hash chains and to authenticate the RSS readings, each node must first distribute the h_n value to its 1-hop neighbors. Usually a trusted certification authority is used to distribute h_n elements in the network; however, due to the distributed architecture and open nature of mobile ad hoc networks this is rarely a possibility. In our scheme, we presume that there are pre-shared symmetric keys between each pair of nodes. Each node distributes the encrypted h_n directly with its 1-hop neighbors without the use of certification authority. Let's say, node 3 distributes h_n with node 0 before sharing the RSS obtained from its 1-hop neighbors with 0, depicted in Figure 6 above. Before disseminating T, node 3 uses h_i (sequentially) to sign the T, where $0 \leq i < n$. Suppose h_n or h_{i+1} has already been exposed to node 0, i.e. $n = i + 1$. Next, node 3 creates a frame F while attaching T with the next one-way hash chain element, h_i as given below.

$$\mathbb{F}(T < T_r, R_v, R_i, t_i >, h_i, M_{h_{i-1}})$$

The M is called Message Authentication Code (MAC) and it is a hash of T, *i.e.*,

$$MAC[T < T_r, R_v, R_i, t_i >]_{h_{i-1}}$$

Since, h_{i+1} is known to node 0, it calculates and compares $H(h_i)$ with h_{i+1}, if the outcome is a match, the h_i element is accepted in order to indicate that the information has been sent by node 3; in case of unmatched information, it shall be rejected. In order to corroborate the integrity of the frame as well, node 0 must wait for the next frame (in which the next hash chain h_{i-1} will be disclosed). Upon the disclosure of h_{i-1}, node 0 will be able to validate the integrity of the previously received frame by computing the MAC and comparing it with the already received one. This is an efficient technique for checking the integrity of information, called the ''delayed disclosure'' technique proposed by [41].

V. SIMULATION RESULTS AND DISCUSSIONS

A. SIMULATION SETUP

We use NS-2.30 network simulator to evaluate our proposed technique using the parameters given in Table 3. The aim of the simulation based evaluation is to establish the detection accuracy of our scheme under different scenarios. After thorough analysis we select some attributes which may affect the detection accuracy of our scheme namely mobility, number of connections, node density, and number of malicious nodes. Throughout the simulation we use speed (mobility) our main parameter. All of the results were obtained as mean of the 25 random seeds.

TABLE 3. Simulation parameters.

Parameter	Level
Area	1000m × 1000m
Speed	0 to 12 m/s
Pause Time	60 s
Radio Propagation Model	Two-ray Ground Reflection
Radio Range	250m
Carrier Sense Range	550m
Number of Nodes	50
MAC	802.11
Application	CBR
Packet Size	64 B
Simulation Time	900s
Movement	Random Waypoint Model
Placement	Uniform
Masqueraders' Population	10%
RSS_TIMEOUT	100 seconds
RSS linked records	5

In the Table 3, by the ''RSS linked records'' we mean the maximum number of collected RSS retained for each identity in the table, as shown in Table 1 above. The number of (linked list) retained RSS records can be adjusted as per the storage requirements, however, the value selected in Table 3 produces good performance during simulations. The RSS_TIMEOUT threshold is used by each node to flush the RSS table from stale entries. If a node does not hear from another node within a stipulated time then it is believed that the node left the network.

B. METRICS

Our main concern is to determine the detection accuracy of our proposed scheme in various environments and in different conditions, so our main metrics will be False Positive Rate (FPR) and True Positive Rate (TPR). By FPR, we mean number of legitimate or innocent nodes that are incorrectly detected as masquerader and TPR is the number of malicious nodes that are correctly detected, as given below.

$$TPR = \frac{\%\ of\ Detected\ masquerading\ ids}{Total\ masquerading\ ids}$$

$$FPR = \frac{\%\ of\ detected\ innocent\ ids\ as\ malicious}{Total\ innocent\ ids}$$

We take both TPR and FPR values in percentages, as shown in the figures given in the following sub-sections.

C. RESULTS ANALYSIS

Throughout our simulation experimentations, in addition to other attributes, such as node density, connections, and number of malicious nodes, we select mobility (speed) as our main parameter for the overall assessment of the scheme. Before, we discuss the other attributes it is important that we discuss the affect of mobility in general. We observe the following. Firstly, in the static case (no mobility), true positives are normally less than that of the mobile case, as shown by all of the TPRs. There are two reasons for it.

- The attacker(s) happen to be deployed randomly in a region with no monitoring nodes at all; hence, these nodes are not detected over the whole simulation time.
- The attacker and the victim node happen to be deployed at about same distance from a monitoring node; hence, the monitoring node does not detect any significant change in the RSS received and the attacker goes undetected.

Secondly, it is also observed that at high mobility the TPR drops a little bit. It is due to the fact that the attacker nodes are not detected if the attacker and the victim both move in almost opposite directions; hence, little change in RSS is detected at the monitoring nodes. Third, in some cases, such as Figure 7(a), increase in mobility induces more false positives. One reason for this may be that when a legitimate node and the detector node move at 180 degree angle with high speed, the detector will observe significant change and the normal node will be deemed as masquerader; hence, an ensued false positive.

As shown in Figure 7, the scheme is evaluated for different node densities and speeds. Node densities have more effect on the FPR than the TPR. It is due to the fact that with high node density (given constant attackers' population) the number of evidence collector nodes will increase; hence, if one node, for example, does not capture the change induced by certain angle or speed, the other detector would notice it. Overall, high node densities produce better detection accuracy, i.e., high TPR and low FPR.

Number of network connections has also a role in our detection system; the effect can be seen by Figure 8. The FPR

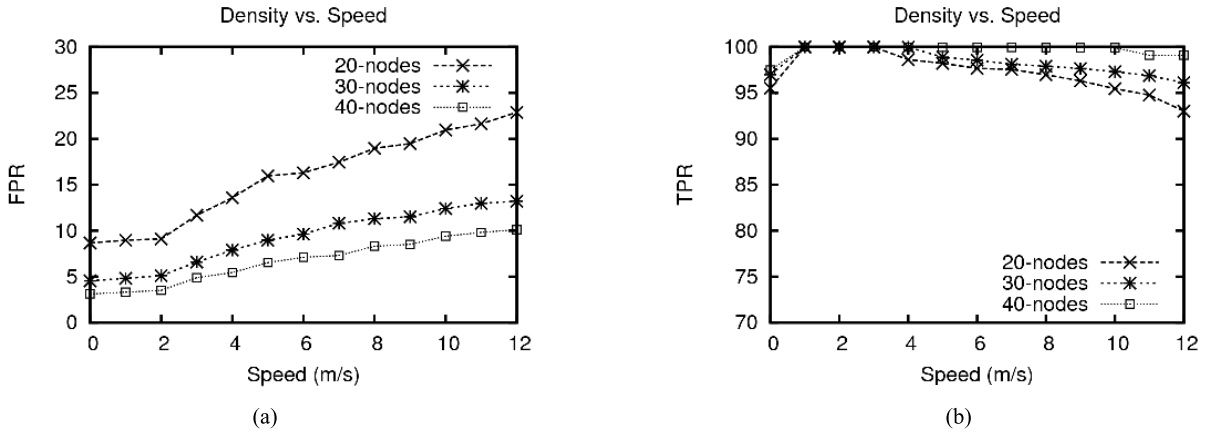

FIGURE 7. (a). FPR and (b) TPR with various node densities and speeds.

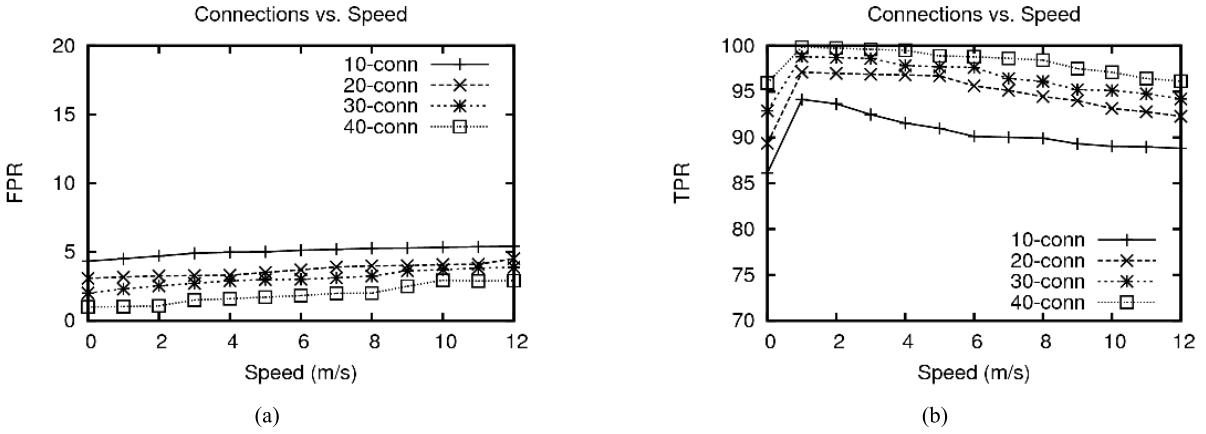

FIGURE 8. (a). FPR and (b) TPR with various network connections and speeds.

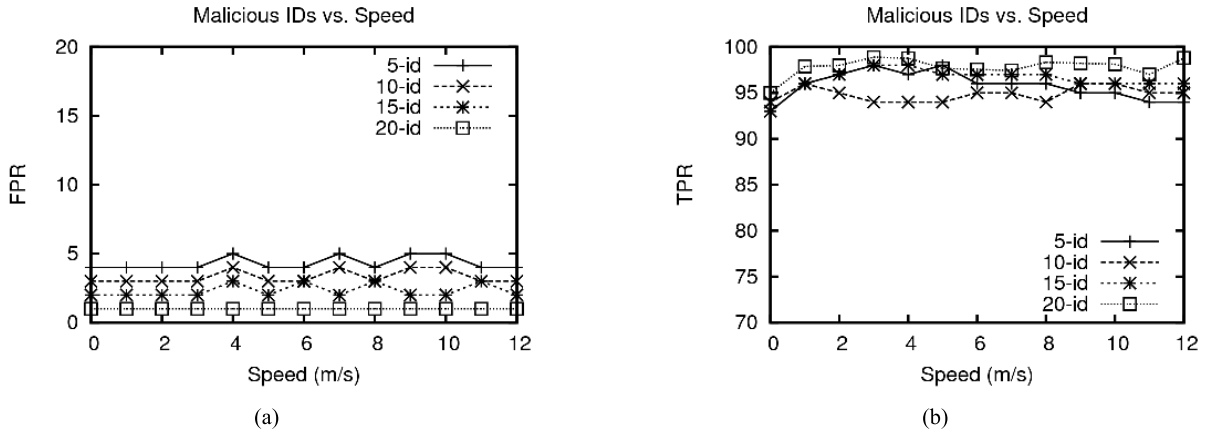

FIGURE 9. (a). FPR and (b) TPR with various masquerader populations and speeds.

is not affected though, but the TPR increases with the increase in the number of connections, as shown in Figure 8(b). The reason for this is that with less number of connections (which is created from random sources to random destinations), some of the attackers may not take part in communication at all, for example, they are not selected as traffic sources, sinks, or forwarders; hence, they go undetected. So the TPR is increased when connections in the network are increased.

In Figure 9, the detection accuracy is assessed with different sets of masqueraders. It is difficult to deduce any trends from the results; however, it is confirmed that in all cases, the FPR is less than 5% whereas the TPR is greater than 90%.

VI. CONCLUSION

In this paper, we designed a model for RSS based detection using null hypothesis and validated it for the detection

accuracy using theoretical RSS variation and real world RSS fluctuation. For real world RSS variation, the experiments were conducted on a testbed of Samsung Galaxy based smartphones. The theoretical model helped us in determining the relationship between the detection accuracy and the distance between the nodes being detected in the presence of variation is the RSS. We then proposed a detection scheme for the masquerading attacks on IEEE 802.11 based ad hoc networks without using any additional hardware or third-party guarantor. Unlike other schemes, our proposed scheme did not use any fixed access point or air monitors. The results obtained indicated good detection accuracy. x

REFERENCES

[1] O. Kaiwartya *et al.*, "Internet of vehicles: Motivation, layered architecture, network model, challenges, and future aspects," *IEEE Access*, vol. 4, pp. 5356–5373, 2016.
[2] S. Jung, H. Cho, D. Kim, K. Kim, J.-I. Han, and H. Myung, "Development of algal bloom removal system using unmanned aerial vehicle and surface vehicle," *IEEE Access*, vol. 5, pp. 22166–22176, 2017.
[3] J. H. Abawajy and H. M. Mehedi, "Federated Internet of Things and cloud computing pervasive patient health monitoring system," *IEEE Commun. Mag.*, vol. 55, no. 1, pp. 48–53, Jan. 2017.
[4] S. Li, L. Da Xu, and S. Zhao, "5G Internet of Things: A survey," *J. Ind. Inf. Integr.*, vol. 10, pp. 1–9, Jun. 2018.
[5] A. Gatouillat, Y. Badr, B. Massot, and E. Sejdić, "Internet of medical things: A review of recent contributions dealing with cyber-physical systems in medicine," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2849014.
[6] S. Xu, Y. Li, Y. Gao, Y. Liu, and H. Ga anin, "Opportunistic coexistence of LTE and WiFi for future 5G system: Experimental performance evaluation and analysis," *IEEE Access*, vol. 6, pp. 8725–8741, 2018.
[7] J. R. Douceur, "The Sybil attack," in *Proc. 1st Int. Workshop Peer-to-Peer Syst.*, 2002, pp. 251–260.
[8] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis & defenses," presented at the 3rd Int. Symp. Inf. Process. Sensor Netw. (IPSN), 2004.
[9] S. Abbas, M. Merabti, D. Llewellyn-Jones, and K. Kifayat, "Lightweight Sybil attack detection in MANETs," *IEEE Syst. J.*, vol. 7, no. 2, pp. 236–248, Jun. 2013.
[10] L. Ma, "Detecting masqueraders in 802.11 wireless networks," in *Proc. Int. Conf. Wireless Netw.*, 2011, pp. 267–271.
[11] S. Misra, A. Ghosh, A. P. Sagar P., and M. S. Obaidat, "Detection of identity-based attacks in wireless sensor networks using signalprints," in *Proc. IEEE/ACM Int. Conf. Green Comput. Commun., Int. Conf. Cyber, Phys. Social Comput.*, Dec. 2010, pp. 35–41.
[12] J. Yu, E. Kim, H. Kim, and J. Huh, "A framework for detecting MAC and IP spoofing attacks with network characteristics," in *Proc. Int. Conf. Softw. Secur. Assurance*, Aug. 2016, pp. 49–53.
[13] Y. Chen, J. Yang, W. Trappe, and R. P. Martin, "Detecting and localizing identity-based attacks in wireless and sensor networks," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2418–2434, Jun. 2010.
[14] Y. Sheng, K. Tan, G. Chen, D. Kotz, and A. Campbell, "Detecting 802.11 MAC layer spoofing using received signal strength," in *Proc. 27th IEEE Conf. Comput. Commun.*, Apr. 2008, pp. 1768–1776.
[15] K. Hoeper and G. Gong, "Bootstrapping security in mobile ad hoc networks using identity-based schemes," in *Security in Distributed and Networking Systems* (Computer and Network Security). Singapore: World Scientific, 2007.
[16] S. Hashmi and J. Brooke, "Towards Sybil resistant authentication in mobile ad hoc networks," in *Proc. 4th Int. Conf. Emerg. Secur. Inf. Syst. Technol. (SECURWARE)*, Jul. 2010, pp. 17–24.
[17] M. N. Mejri, J. Ben-Othman, and M. Hamdi, "Survey on VANET security challenges and possible cryptographic solutions," *Veh. Commun.*, vol. 1, no. 2, pp. 53–66, Apr. 2014.
[18] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)," *Wireless Netw.*, vol. 24, no. 2, pp. 373–382, 2018.
[19] K. Hamouid and K. Adi, "Efficient certificateless Web-of-trust model for public-key authentication in MANET," *Comput. Commun.*, vol. 63, pp. 24–39, Jun. 2015.
[20] S. Maity and R. C. Hansdah, "Self-organized public key management in manets with enhanced security and without certificate-chains," *Comput. Netw.*, vol. 65, pp. 183–211, Jun. 2014.
[21] A. Seth and S. Keshav, "Practical security for disconnected nodes," in *Proc. 1st IEEE ICNP Workshop Secure Netw. Protocols (NPSec)*, Nov. 2005, pp. 31–36.
[22] M. C. Chuang and J. F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Syst. J.*, vol. 8, no. 3, pp. 749–758, Sep. 2014.
[23] S. Hashmi and J. Brooke, "Authentication mechanisms for mobile ad-hoc networks and resistance to Sybil attack," in *Proc. 2nd Int. Conf. Emerg. Secur. Inf., Syst. Technol.*, Aug. 2008, pp. 120–126.
[24] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks—A survey," *Comput. Commun.*, vol. 51, pp. 1–20, Sep. 2014.
[25] S. Gil, S. Kumar, M. Mazumder, D. Katabi, and D. Rus, "Guaranteeing spoof-resilient multi-robot networks," *Auton. Robots*, vol. 41, no. 6, pp. 1383–1400, 2017.
[26] S. Gilbert, C. Newport, and C. Zheng, "Who are you? Secure identities in single hop ad hoc networks," *Distrib. Comput.*, vol. 30, no. 2, pp. 103–125, 2017.
[27] M. A. Jan, P. Nanda, X. He, and R. P. Liu, "A Sybil attack detection scheme for a forest wildfire monitoring application," *Future Gener. Comput. Syst.*, vol. 80, pp. 613–626, Mar. 2018.
[28] M. Faisal, S. Abbas, and H. U. Rahman, "Identity attack detection system for 802.11-based ad hoc networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2018 , no. 1, p. 128, 2018.
[29] B. N. Levine, C. Shields, and N. B. Margolin, "A survey of solutions to the Sybil attack," Dept. Comput. Sci., Univ. Massachusetts Amherst, Amherst, MA, USA, Tech. Rep. 2006-052, 2006.
[30] S. Abbas, M. Merabti, and D. Llewellyn-Jones, "Signal strength based Sybil attack detection in wireless ad hoc networks," in *Proc. 2nd Int. Conf. Develop. eSyst. Eng. (DESE)*, Dec. 2009, pp. 190–195.
[31] J. Yang, Y. Chen, and W. Trappe, "Detecting spoofing attacks in mobile wireless environments," in *Proc. 6th Annu. IEEE Commun. Soc. Conf. Sensor, Mesh Ad Hoc Commun. Netw.*, Jun. 2009, pp. 1–9.
[32] D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using signalprints," in *Proc. 5th ACM Workshop Wireless Secur.*, 2006, pp. 43–52.
[33] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. Workshop Hot Topics Netw. (HotNets-IV)*, 2005, pp. 1–6.
[34] L. Mengual, O. Marbán, and S. Eibe, "Clustering-based location in wireless networks," *Expert Syst. Appl.*, vol. 37, no. 9, pp. 6165–6175, 2010.
[35] C. Phillips, D. Sicker, and D. Grunwald, "A survey of wireless path loss prediction and coverage mapping methods," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 1, pp. 255–270, 1st Quart., 2013.
[36] H. Nurminen, M. Dashti, and R. Piché, "A survey on wireless transmitter localization using signal strength measurements," *Wireless Commun. Mobile Comput.*, vol. 2017, Feb. 2017, Art. no. 2569645.
[37] D. C. Montgomery and G. C. Runger, *Applied Statistics and Probability for Engineers*. Hoboken, NJ, USA: Wiley, 2010.
[38] T. K. Sarkar, Z. Ji, K. Kim, A. Medouri, and M. Salazar-Palma, "A survey of various propagation models for mobile communication," *IEEE Antennas Propag. Mag.*, vol. 45, no. 3, pp. 51–82, Jun. 2003.
[39] Y. Hu and G. Leus, "Robust differential received signal strength-based localization," *IEEE Trans. Signal Process.*, vol. 65, no. 12, pp. 3261–3276, Jun. 2017.
[40] D. Coppersmith and M. Jakobsson, "Almost optimal hash sequence traversal," in *Proc. Int. Conf. Financial Cryptogr.*, 2002, pp. 102–119.
[41] Y.-C. Hu, D. B. Johnson, and A. Perrig, "SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks," *Ad Hoc Netw.*, vol. 1, no. 1, pp. 175–192, Jul. 2003.
[42] R. L. Rivest, *The MD5 Message-Digest Algorithm*, document RFC 1321, MIT Laboratory for Computer Science and RSA Data Security, 1992.
[43] D. Eastlake and P. Jones, "US secure hash algorithm 1 (SHA1)," Cisco, San Jose, CA, USA, White Paper 2070-1721, 2001.
[44] M. Jakobsson, "Fractal hash sequence representation and traversal," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun./Jul. 2002, p. 437.

SOHAIL ABBAS received the Ph.D. degree in wireless network security from Liverpool John Moores University, U.K., in 2011. He is currently an Assistant Professor with the Department of Computer Science, University of Sharjah, United Arab Emirates. His research interests include security and cooperation enforcement in mobile ad hoc networks. He is a member of a number of technical program committees, including IEEE CCNC, IEEE VTC, IEEE ISCI, and IEEE ISWTA. He is also serving in various prestigious journals as a Reviewer, such as *Security and Communication Networks*, *IET Wireless Sensor Systems*, *Mobile Networks and Applications*, the *International Journal of Electronics and Communications*, and the *International Journal of Distributed Sensor Networks*.

MOHAMMAD FAISAL received the M.S. degree in information management system (network security) from SZABIST, Pakistan, in 2012. He is currently a Lecturer and a Ph.D. Scholar with the Department of Computer Science and Information Technology, University of Malakand. His research interests include security of wireless ad hoc network and digital forensics.

HASEEB UR RAHMAN received the Ph.D. degree in P2P networks from Liverpool John Moores University, U.K., in 2013. He is currently an Assistant Professor with the Department of Computer Science and IT, University of Malakand, Pakistan. He is currently involved in IoT smart farming and Internet of Cultural Things. His research interests include P2P and social P2P networks, MANETs, cloud computing, sensor networks, and IoT. He is also a TPC Member of various conferences, such as IEEE CCNC.

MUHAMMAD ZAHID KHAN received the B.C.S. degree (Hons.) in computer science from the University of Peshawar, Pakistan, in 2003, and the Ph.D. degree from the School of Computing and Mathematical Sciences, Liverpool John Moores University, U.K., in 2013. He has been an Assistant Professor with the Department of Computer and Information Technology, University of Malakand, Pakistan, since 2005, where he is currently leading the Network Systems and Security Research Group, Department of CS and IT. His current research interests include wireless sensor networks, mobile ad hoc networks, and the Internet of Things. He is a Higher Education Commission's Pakistan Approved Supervisor.

MADJID MERABTI received the degree from Lancaster University, U.K. He was the Dean of the School of Computing and Mathematical Sciences, Liverpool John Moores University, U.K., and the Director of the Research Centre for the Protection of Critical Infrastructure. He is currently a Professor of networked and security systems and the Dean of the College of Sciences, University of Sharjah, United Arab Emirates. He has over 30 years' experience in conducting research and teaching in the areas of computer networks (fixed and wireless), computer network security, digital forensics, multimedia, games technology, and their applications. He has widely published over 300 publications in these areas and leads a number of EU, U.K., and industry-supported research projects. He is a frequent Keynote Speaker at major international conferences in his research areas and an Editor of the *IEEE Communications Magazine* Home Networking Series. He is a Co-Editor-in-Chief of the *International Journal of Pervasive Computing and Communications*. He is also an Associate Editor of *Computer Communications* journal (Elsevier), the *Journal of Security and Communication Networks* (Wiley), the *Peer-to-Peer Networking and Applications Journal* (Springer), the *Advances in Multimedia Journal*, and the *Journal of Computer Systems, Networks and Communication* (Hindawi Publishing). He is a member and the chair of a number of conference TPCs and the Chair of the Post Graduate Networking Symposium series for U.K. Ph.D. students.

ATTA UR REHMAN KHAN was the Director of the National Cybercrime Forensics Lab Pakistan, the Head of the Air University Cybersecurity Center, and the Conferences Chair of the IEEE Islamabad Section. He is currently an Associate Professor with the Faculty of Computing and Information Technology, Sohar University, Oman. His areas of research interest include cybersecurity, mobile cloud computing, ad hoc networks, and IoT. He is a Steering Committee Member/Track Chair/Technical Program Committee (TPC) Member of over 60 international conferences. He also serves as a Domain Expert for multiple international research funding bodies and has received multiple awards, fellowships, and research grants. He is currently serving as an Associate Editor of the IEEE Access and the *Journal of Network and Computer Applications* (Elsevier), an Associate Technical Editor of the *IEEE Communications Magazine*, and an Editor of the *Journal of Cluster Computing* (Springer), *The Computer Journal* (Oxford), the IEEE SDN Newsletter, the *KSII Transactions on Internet and Information Systems*, *Human-centric Computing and Information Sciences* (SpringerOpen), *SpringerPlus*, and *Ad Hoc and Sensor Wireless Networks* journal. For more updated information, visit his website at www.attaurrehman.com.